



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/892,310	06/26/2001	Zheng Qi	2875.0450001	2328

26111 7590 12/06/2006

STERNE, KESSLER, GOLDSTEIN & FOX PLLC
1100 NEW YORK AVENUE, N.W.
WASHINGTON, DC 20005

EXAMINER

SHIFERAW, ELENI A

ART UNIT	PAPER NUMBER
----------	--------------

2136

DATE MAILED: 12/06/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/892,310	Applicant(s) QI ET AL.	
	Examiner Eleni A. Shiferaw	Art Unit 2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 31 August 2006.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 3,5-8,11-14,16-21,46,48-54 and 68-79 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☒ Claim(s) 80 is/are allowed.
- 6) ☒ Claim(s) 3, 5-8, 11-14, 16-21, 46, 48-54, and 68-79 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|---|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date <u>08/31/2006</u> | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 08/31/2006 has been entered.

Applicant's amendments necessitated an election/restriction requirement due to newly added claims.

Information Disclosure Statement

2. Documents listed in the IDS submitted by applicant on 8/8/2006 have been considered.

Response to Arguments

3. Applicant's amendments and arguments with respect to claim 3, 5-8, 11-14, 16-21, 46, 48-54, and 68-79 have been considered but are moot in view of the new ground(s) of rejection.

Election/Restrictions

4. Retraction to one of the following inventions is required under 35 U.S.C. 121:

I. Claims 3, 5-8, 11-14, 16-21, 46, 48-54, and 68-79, are drawn to an encryption apparatus, classified in class 380, subclass 37.

II. Claim 80, is drawn to an encryption method, classified in class 380, subclass 28. The inventions II and I are related as process and apparatus for its practice. The inventions are distinct if it can be shown that either: (1) the process as claimed can be practiced by another and materially different apparatus or by hand, or (2) the apparatus as claimed can be used to practice another and materially different process. (MPEP 806.05(e)). In this case the method can be performed by a materially different apparatus than invention I.

Because these inventions are independent or distinct for the reasons given above and have acquired a separate status in the art in view of their different classification restriction for examination purposes as indicated is proper.

During telephone conversation with Ms. Lori Gordon on 8/9/2006 a provisional election was made without traverse to prosecute the invention of group I, claims 3, 5-8, 11-14, 16-21, 46, 48-54, and 68-79. Affirmation of this election must be made by applicant in replying to this Office action. **Claim 80 is withdrawn from further consideration by the examiner, 37 CFR 1.142(b), as being drawn to a non-elected invention.**

Applicant is reminded that upon the cancellation of claims to a non-elected invention, the inventorship must be amended in compliance with 37 CFR 1.48(b) if one or more of the currently named inventors is no longer an inventor of at least one claim remaining in the application. Any amendment of inventorship must be accompanied by a request under 37 CFR 1.48(b) and by the fee required under 37 CFR 1.17(i).

Claim Rejections - 35 USC § 112

5. The following is a quotation of the second paragraph of 35 U.S.C. 112:

Art Unit: 2136

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 3, and 46 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claims 3 and 46 define the cryptography engine of claim 68 as a DES engine. The examiner notes that an engine of the data encryption standard has a well known structure. See further, Figure 12.2 on p272 of Schneier, which discloses a standard DES engine. While one of ordinary skill in the art would recognize that the majority of what is recited in claim 68 belongs to a DES engine, claim 68 also has the extra component of the “ ‘means for combining’ or ‘a second XOR logic’, as recited in claims 68 and 73, respectively, via a second logic operation the third bit sequence with the second inverse permuted bit sequence to generate a fourth bit sequence”. This extra component means that the cryptography engine of claims 68 and 73 is an improvement upon DES engine. As such, because of the improvement, one can no longer claim that the engine is a DES engine since DES is a standard. One cannot improve upon a standard and still say that what results is the same standard. Note that there is no XOR before the final permutation in a standard DES engine.

Double Patenting

6. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the “right to exclude” granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined

Art Unit: 2136

application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

Claims 3, 5-8, 11-14, 16-21, 46, 48-54, and 68-79 are provisionally rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 1, 3-8, 13-19, 21, 23, 25-34, 36, 38-42 of copending Application No. 09/892,242.

Claim(s) 1 and 4 of provisional application 09/892,242 contain(s) every element of claim(s) 68 of the instant application and as such anticipate(s) claim(s) 3, 5-8, 11-14, 16-21, 46, 48-54, and 68-79 of the instant application, as underlined and shown in the table below.

Instant application 09/892,310	Copending application 09/892,242
<p>68. A cryptography engine for performing cryptographic operations on a data block having a first portion and a second portion, the cryptography engine comprising:</p> <p style="padding-left: 40px;">a key scheduler configured to provide a plurality of keys for cryptographic operations;</p> <p style="padding-left: 40px;">means for combining via a first logical operation one of the plurality of keys provided by the key scheduler with a first bit</p>	<p>1. A cryptography engine for performing cryptographic operations on a data block, the cryptography engine comprising:</p> <p style="padding-left: 40px;">a key scheduler configured to provide keys for cryptographic operations;</p> <p style="padding-left: 40px;">expansion logic configured to expand a first bit sequence having a first size to an expanded first bit sequence having a second size greater than the first size, the first bit sequence corresponding to a right portion of an input bit sequence for the current cryptographic round;</p> <p style="padding-left: 40px;">first circuitry configured to perform an</p>

Art Unit: 2136

sequence to generate a second bit sequence, wherein the first bit sequence is an expansion of the first portion of the data block;

substitution logic for receiving the second bit sequence and for generating a third bit sequence;

a first inverse permutation logic for performing, during an initial cryptographic round, an inverse permutation of the first portion of the data block and for generating a first inverse permuted bit sequence, wherein the first inverse permuted bit sequence is a first input bit sequence for a subsequent cryptographic round;

a second inverse permutation logic for performing, during an initial cryptographic round, an inverse permutation of the second portion of the data block and for generating a second inverse permuted bit sequence;

means for combining via a second logic operation the third bit sequence with the second inverse permuted bit sequence to generate a fourth bit sequence; and

a permutation logic for permuting the fourth bit sequence and generating a permuted bit sequence, wherein the permuted bit sequence is a second input bit sequence for the subsequent cryptographic round.

exclusive OR(XOR) on the expanded first bit sequence and a key provided by the key scheduler to generate a third bit sequence;

a substitution box (Sbox) configured to transform the third bit sequence into a fourth bit sequence;

second circuitry configured to perform an exclusive OR (XOR) on the fourth bit sequence and a left portion of the input bit sequence for the current cryptographic round to generate a fifth bit sequence;

permutation logic coupled to the expansion logic and the second circuitry, the permutation logic configured to receive the fifth bit sequence from the second circuitry and to perform a permutation of the fifth bit sequence,

wherein the fifth bit sequence is a right portion of an output bit sequence of a current cryptographic round.

4. The cryptography engine of claim 1, further comprising two-level multiplexer circuitry, wherein a first level of the two-level multiplexer is configured to receive an inverse permutation of a first portion of the input bit sequence and an inverse permutation of a second portion of the input bit sequence during an initial cryptographic round and a right portion of an output bit sequence from a previous cryptographic round during a subsequent cryptographic round and wherein a second level of the two-level multiplexer is configured to receive the output of the first level and the right portion of the output bit sequence generated during the previous cryptographic round.

“A later patent claim is not patentably distinct from an earlier patent claim if the later claim is obvious over, or **anticipated** by, the earlier claim. In re Longi, 759 F.2d at 896, 225 USPQ at

Art Unit: 2136

651 (affirming a holding of obviousness-type double patenting because the claims at issue were obvious over claims in four prior art patents); In re Berg, 140 F.3d at 1437, 46 USPQ2d at 1233 (Fed. Cir. 1998) (affirming a holding of obviousness-type double patenting where a patent application claim to a genus is anticipated by a patent claim to a species within that genus). “ELI LILLY AND COMPANY v BARR LABORATORIES, INC., United States Court of Appeals for the Federal Circuit, ON PETITION FOR REHEARING EN BANC (DECIDED: May 30, 2001).

This is a provisional obviousness-type double patenting rejection because the conflicting claims have not in fact been patented

Allowable Subject Matter

7. The following is a statement for reasons for the indication of allowable subject matter: As per claims 68, 73, and 78 most of the limitations claimed are found in DES engine, for example: the key scheduler, the expansion logic, the first circuitry, the substitution box, and the permutation logic. However, the prior art of record fails to teach “a second XOR logic combiner via a second logic operation the third bit sequence with the second inverse permuted bit sequence to generate a fourth bit sequence”

Claims 3, 5-8, 11-14, 16-21, 46, 48-54, and 68-79 would be allowable if amended and/or file terminal disclaimer for obviousness type double patenting rejection, set forth in this Office action.

Claims 3 and 46 would be allowable if rewritten or amended to overcome the rejection(s) under 35 U.S.C. 112, 2nd paragraph, set forth in this Office action.

Conclusion

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Eleni A. Shiferaw whose telephone number is 571-272-3867.

The examiner can normally be reached on Mon-Fri 8:00am-5:00pm.


If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser R. Moazzami can be reached on (571) 272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.



November 21, 2006

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100


11/24/06